AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Bryan J. Wilmot, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— four electronic devices as described in Attachment A—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service, and have been so employed since March 4, 2018. I am currently assigned to the Manchester, New Hampshire Resident Office. In preparation for my employment with the Secret Service, I completed training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as at the Secret Service's James J. Rowley Training Center in Laurel, Maryland. In addition to these training programs, I have completed numerous in-service training courses related to constitutional law, and was a federal police officer for approximately 3 years prior to becoming a Special Agent. My present duties include the investigation of federal offenses, including, but not limited to, those involving financial fraud and its related activities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is a silver-colored Apple iPhone, model number A1549, IMEI #358373068022358; a white Apple iPhone, with no externally-printed model

number or IMEI; a black Seagate portable hard drive, model number SRD00F1, serial number NA42JWSK; and a white SIM/Micro Chip, serial number 8901260955180336076 – hereinafter the "Devices." The Devices are currently located in the custody of the U.S. Secret Service at 1000 Elm Street, Manchester, New Hampshire 03101.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On Monday, June 3, 2019, Brad Barbin, Vice President of Federal Savings Bank (FSB), contacted the U.S. Secret Service in Manchester, New Hampshire regarding transactions conducted at FSB ATMs with fraudulent ATM cards. He explained that the criminal activity involved the use of Dunkin Donuts gift cards, reencoded with bank account information, to conduct fraudulent cash withdrawals at six FSB locations in Barrington, Dover, Durham, Portsmouth, and Rochester, New Hampshire. The suspects' activity resulted in an initial suspected loss of approximately $40,000, and was conducted over three distinct time periods: April 27 through April 30, May 11 through May 12, and May 25 through May 28, 2019.

7. On Friday, June 7, 2019, I responded to the FSB branch in Dover, New Hampshire where Mr. Barbin provided copies of pictures taken from the FSB ATM cameras during the unauthorized transactions. The pictures showed various individuals making transactions between the dates of April 27 and May 31 that FSB identified as possible fraud. One white male of medium build appeared consistently across the three distinct periods of suspected fraudulent activity. This unidentified male was the driver of the vehicle during the initial two periods, and then alternated as the driver and passenger during the third period with another unidentified white male. This second suspect was also of medium build, had a thin dark-

colored beard, and wore a dark colored baseball cap. From the provided ATM footage, I was also able to view the license plate for the vehicle used during the third week of activity – a black Toyota Yaris with Massachusetts license plate 4CW349.

8. Continuing on June 7, 2019, Detective Katie Bolton of the Durham Police Department forwarded the results of her vehicle registration database check on the Toyota Yaris, which showed that the car belonged to Different Auto Service, LLC, a rental car company based in Natick, Massachusetts. The owner of the company, Maria Damota, forwarded Detective Bolton a copy of the rental agreement and pictures of the identification provided by the renters. Ms. Damota confirmed that the men who rented the vehicles matched the pictures on the identification. The renters were identified as Ricardo Augusto Dos Santos (DOB: [redacted]) and Estefano Dall Anese Borlotti (DOB: [redacted]). Dos Santos had provided his Florida driver's license to rent the vehicle, and Borlotti his Brazilian driver's license and Brazilian passport. Upon review of the copies of the photographs, I confirmed that the pictures matched the identities of the individuals on the ATM cameras, with Dos Santos being the suspect seen across all three periods of activity, and Borlotti being the one with whom he alternated driving during the third period. The vehicle was rented on May 25, 2019 and returned on May 28, 2019.

9. Continuing on June 7, 2019, inquiries with the Department of Homeland Security (DHS) resulted in an immigration photograph of Borlotti, which matched the picture on the Brazilian driver's license and Brazilian passport he provided, as well as the pictures of the second individual seen conducting fraudulent ATM transactions.

10. On Monday, June 24, 2019, Nicole Huntress, Operations Manager of Holy Rosary Credit Union (HRCU), contacted the Secret Service in Manchester to report fraud that took place at five HRCU branch locations in Dover, Farmington, and Rochester, New Hampshire. The

fraud took place from May 25 through May 28, 2019, and again from June 19 through June 23, 2019. ATM footage revealed both Dos Santos and Borlotti again using Dunkin Donuts gift cards to fraudulently withdraw money from ATMs, with initial loss estimates of approximately $42,000. In one picture from a transaction attempt on June 21, 2019, Borlotti can be seen taking a photograph of the ATM with his phone, while in other video the suspects can be seen referring to their phones while conducting their transactions.

11. Between late April and June, Borlotti and Dos Santos are believed to have left the New Hampshire area, and Borlotti returned to Brazil. Our investigation continued.

12. To determine the source from which the suspects obtained their bank account information, I contacted Charles Schwab – the issuing bank of at least seven compromised accounts that had been used to commit fraudulent transactions. I asked Chris Rolls, financial investigator for Charles Schwab, to review the transaction and account history for each compromised account to identify a common point of compromise.

13. I know from my training and experience that a common point of compromise is a single location at which multiple compromised accounts all conducted some form of financial transaction. By identifying this point, it can reveal how the legitimate account holders' information was originally stolen, and thus later used to commit fraud. I also know from my training and experience that a compromised account number can be saved on a variety of electronic storage devices, to include cellular telephones, hard drives, and SIM/Micro Chips, to be loaded at a later time onto gift cards. The act of then loading the compromised account onto a gift card can be accomplished in a variety of methods, to include a commercially available application on a cellular telephone.

14. Continuing on Tuesday, September 10, 2019, Chris Rolls called to say that he had identified a common usage history among the seven card numbers I provided him. All seven cards had been used at ATMs in Sao Paulo, Brazil between January and June, 2019, and all seven cards had been used to withdraw money at either FSB or HRCU ATMs. Rolls confirmed that each transaction had been reported as fraud, and the financial losses suffered by FSB and HRCU.

15. On Thursday, October 24, 2019, Borlotti arrived at Miami International Airport on American Airlines flight 930 from Sao Paulo, Brazil. There, he was stopped by Customs and Border Protection Officers on a travel alert notice and referred to secondary screening. During secondary screening, it was found that Borlotti had in his possession two (2) reencoded credit cards, and the aforementioned four Devices:

- Silver-colored Apple iPhone, model number A1549, IMEI #358373068022358
- White Apple iPhone, with no externally-printed model number or IMEI
- Black Seagate portable hard drive, model number SRD00F1, serial number NA42JWSK
- White SIM/Micro Chip, serial number 8901260955180336076

16. Based on my training and experience, I know that fraudulent ATM withdrawals are often done through the use of stolen bank card information that is encoded into another card for use. As mentioned above, this case involved the misuse of Dunkin Donut gift cards at ATMs in New Hampshire. I know that the account information needed to accomplish such a scheme can be transported electronically on portable electronic media such as the Devices.

17. Continuing on Thursday, October 24, 2019, Miami-Dade Police Department Detective Marcos Rodriguez arrested Borlotti for violations of Florida statutes for Trafficking or

Possession of Counterfeit Credit Cards, Organized Scheme to Defraud, and Forgery of Credit Card with Intent to Defraud. Homeland Security Investigations (HSI) Special Agent Tony Praznik seized the Devices as evidence and began a search of them in accordance with HSI's warrantless border search authority.

18. On October 30, 2019, a federal grand jury sitting in Concord, New Hampshire returned an indictment against Dos Santos, Borlotti, and a third individual, Juan Cunda, charging them with conspiracy to commit bank fraud based on the aforementioned fraudulent ATM transactions identified above. Federal arrest warrants were then issued, and Borlotti was taken into federal custody in Florida on or about November 18, 2019. He has since been transferred to the District of New Hampshire.

19. Based on Borlotti's residence in Sao Paulo, Brazil, travel to and from the United States from Sao Paulo, arrest at Miami International Airport on a flight from Sao Paulo, and subsequent fraudulent withdrawals of cash using bank cards compromised in Sao Paulo, there is probable cause to believe that the Devices contain evidence of criminal activity in violations of Title 18 U.S.C. § 1344 – Bank Fraud and Title 18 U.S.C. § 1349 – Conspiracy to Commit Bank Fraud.

20. The Devices are currently in the possession of the U.S. Secret Service in the District of New Hampshire. They came into the Secret Service's possession in the following way: On Thursday, October 24, 2019, Borlotti was arrested by Miami-Dade Police Department and his Devices seized by Homeland Security Investigations Special Agent Tony Praznik. The Devices were later retrieved from HSI custody by U.S. Secret Service Special Agent Tyler Bandurski of the Miami Field Office on Thursday, November 21, 2019. On Monday, December 23, 2019, the Devices arrived via UPS to the Manchester Resident Office. Therefore, while the

Secret Service may already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

21. The Devices are currently in U.S. Secret Service storage at 1000 Elm St, Manchester, NH, 03101. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Secret Service.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing

and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS, and PDA. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the

criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Bryan J. Wilmot
Bryan J. Wilmot
Special Agent
United States Secret Service

Subscribed and sworn to before me
on January 13, 2020

/s/ Andrea K. Johnstone
Hon. Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

The property to be searched is a silver-colored Apple iPhone, model number A1549, IMEI #358373068022358; a white Apple iPhone, with no externally-printed model number or IMEI; a black Seagate portable hard drive, model number SRD00F1, serial number NA42JWSK; and a white SIM/Micro Chip, serial number 8901260955180336076 – hereinafter the "Devices." The Devices are currently located in the custody of the U.S. Secret Service at 1000 Elm Street, Manchester, New Hampshire 03101.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18 U.S.C. § 1344 – Bank Fraud and Title 18 U.S.C. § 1349 – Conspiracy to Commit Bank Fraud and involve Borlotti, including:

   a. lists of customers and related identifying information;

   b. types, amounts, prices, dates, places, and amounts of specific transactions;

   c. any information related to sources of obtained victim financial information (including names, addresses, phone numbers, or any other identifying information);

   d. any information recording Borlotti's schedule or travel

   e. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.